Table des matières

Chiffrement et signatures électroniques

Principe des clefs asymétriques

Le principe des clefs asymétriques est simple.

Supposons deux interlocuteurs dialoguant par courriel. L'un est l'émetteur (noté É), l'autre le récepteur (noté R). R possède un jeu de deux clefs dîtes clé publique (notée K_b) et clé privée (notée K_v). Ces deux clés fonctionnent ensembles. Elles seront utilisées l'une pour chiffrer (K_b), l'autre pour déchiffrer (K_v)[1].

É souhaite envoyer un courriel à R. Ce dialogue doit revêtir un caractère confidentiel et aussi bien É que R souhaitent chiffrer cette correspondance afin que personne ne puisse connaître le contenu de ce dialogue. Nous savons (ou pas) que certains facteurs sont très curieux. C'est par exemple le cas de certains fournisseurs de courriel comme gmail qui lisent et enregistrent le contenu des correspondances. Nous ne savons pas ce qu'il advient de ces contenus. Peuvent-ils être transmis à des assureurs santé qui auront déduit que vous êtes malade et ajusteront votre cotisation à certains critères ?

1 Wikipédia : cryptographie asymétrique

É va donc chiffrer le courriel. Pour chiffrer ce courriel, il utilisera la clé publique de R (K_{bR}). Cette clef publique lui aura été transmise directement par R ou via un organisme certificateur (nous reviendrons sur cet aspect dans le chapitre « Vérification et certificats ». Seul R pourra déchiffrer le courriel de É car, pour déchiffrer, il faudra avoir la clé privée K_{vR} associée à la clé publique K_{bR}.

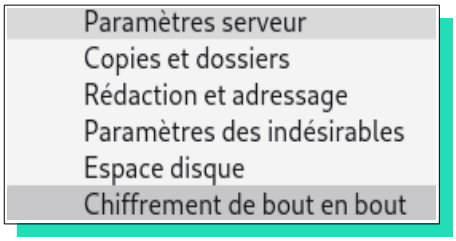
Une personne souhaitant engager un dialogue chiffrée devra donc posséder une paire de clés associées (clé privée, clé publique). Il transmettra sa clé publique à ses interlocuteurs potentiels qui pourront chiffrer les courriels à son attention et pourra les déchiffrer avec sa clé privée qu'il ne transmettra sous aucun prétexte.

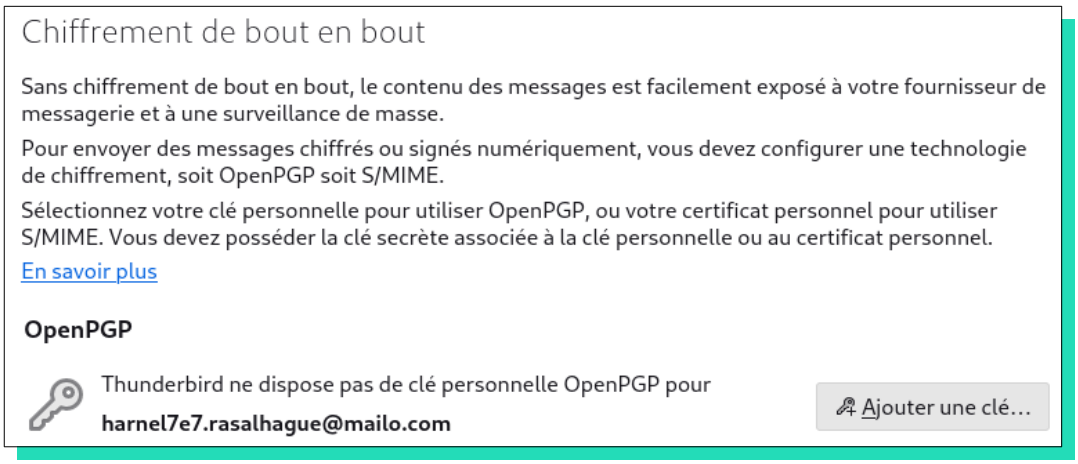
Signalons que cette paire de clé pourra également être utilisée pour la signature électronique. Cela est rendu possible car les clés sont interchangeables. La clé privée peut être utilisée pour chiffrer et la clé publique pour déchiffrer. Nous verrons comment faire dans le chapitre Signature électronique.

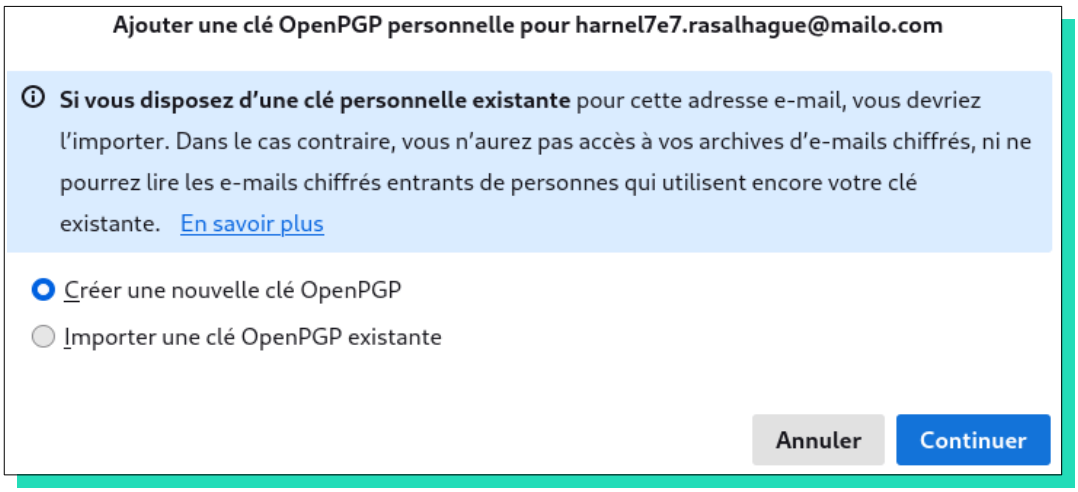
Création de clefs sous thunderbird

Génération d'une paire de clefs (clés publiques et privées)

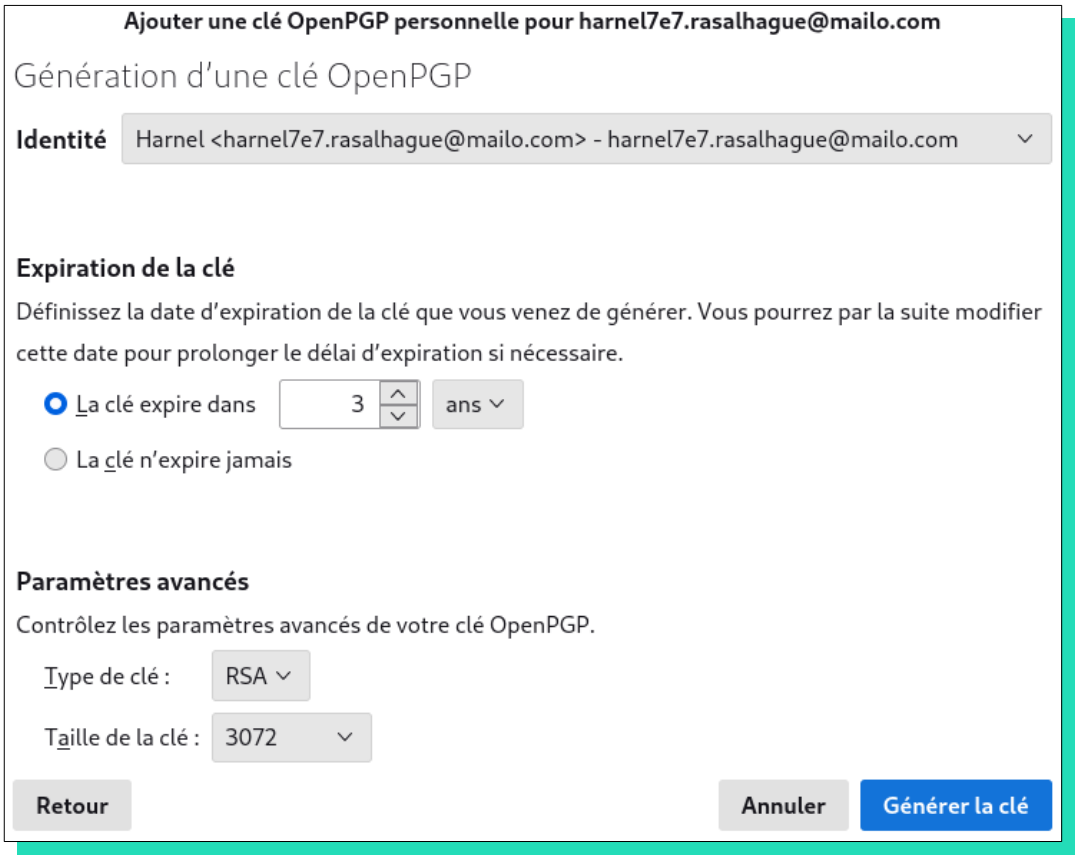
La première étape consiste donc à créer une paire de clés associées l'une à l'autre. Nous utiliserons pour ce faire le logiciel de messagerie électronique thunderbird. Sous l'option de menu « *Édition / paramètres des comptes* », vous sélectionnez « *Chiffrement de bout en bout* » sur l'adresse courriel pour laquelle vous souhaitez créer une paire de clés.





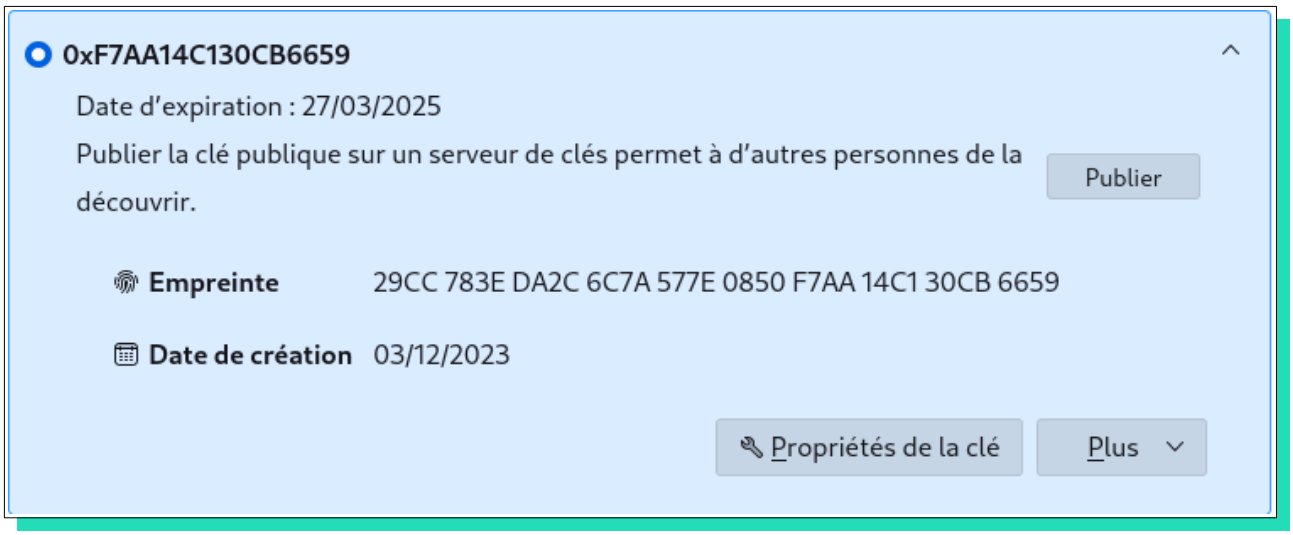


En cliquant ensuite sur « *Ajouter une clé …* », vous pouvez demander la création d'une paire de clés puis la paramétrer en précisant sa durée de validité puis le type et la taille du chiffrement.



Par exemple, votre serviteur change d'adresse tous les ans pour éviter les spams. Une nouvelle paire de clés est créée chaque année et associée à chaque nouvelle adresse et n'est donc valide que 16 mois.

Publication sur un serveur de clefs



Nous verrons dans le chapitre suivant que cette technique, aussi sûre qu'elle paraisse peut cependant être piratée par l'homme du milieu. Afin de contrer ce type de piratage, il est conseillé de publier notre clé vers un serveur de clefs. Thunderbird propose donc cette publication. Par ailleurs, cela permet de faire connaître notre clef publique aux éventuels interlocuteurs qui voudraient chiffrer des courriels à notre intention. Le dialogue précédent poursuit donc cet objectif.

Piratage des clefs asymétriques ?

Il est quasiment impossible de connaître l'autre composante d'une clef asymétrique, quelque soit le type de chiffrement (cryptographie à clef publique, cryptographie homomorphe ou cryptographie à courbes elliptiques). Nous pourrions donc penser nous sentir à l'abri de pirates mais c'est sans compter sur l'homme du milieu capable de déjouer ces systèmes.

Le principe de piratage est le suivant :

Lors d'un dialogue entre émetteur et récepteur, le pirate appelé « *homme du milieu*[2] » car il se place au centre de la conversation. Il se fait passer comme l'émetteur vis à vis du récepteur et pour le récepteur vis à vis de l'émetteur.

Il possède deux paires de clés : une paire pour dialoguer avec l'émetteur et une autre paire pour dialoguer avec le récepteur.

Il transmet sa clé publique version récepteur à l'émetteur en se faisant passer pour le récepteur. Les informations chiffrées par l'émetteur le sont donc avec une fausse clé publique que le pirate peut déchiffrer car il possède la clé privée associée.

2 https://fr.wikipedia.org/wiki/Attaque_de_l%27homme_du_milieu

Il peut ensuite transmettre le message de l'émetteur au récepteur via la clé publique du récepteur à qui il aura par ailleurs transmis son autre clé publique, celle qui lui permet de se faire passer pour l'émetteur.

Le message transmis pourra être ou non altéré selon les objectifs du pirate. Le message ne sera pas altéré si le pirate souhaite simplement recueillir des informations.

Vérification et certificats

Il y a au moins deux parades à ce piratage :

- La première consiste à l'échange en présentiel des clés publiques entre émetteur et récepteur (par exemple via une clé USB). Un homme du milieu dialoguant avec des clés publiques différentes ne pourra déchiffrer les conversations.
- Mais l'échange en présentiel n'est pas toujours possible. Les clés publiques seront alors certifiés par un organisme certificateur à qui nous aurons préalablement transmis notre clé publique. Souvenez-vous que thunderbird a enregistré notre clé publique lors de sa création auprès d'un serveur de clés. Nous pouvons d'ailleurs vérifier auprès du serveur de clés si notre clé est bien référencée après publication[3].

Signature électronique

Au début de cet article, nous avons précisé que nos clés sont interchangeables. Nous allons utiliser cette propriété pour signer numériquement nos courriels.

Le principe de la signature électronique est le suivant :

Nous rédigeons un courriel avec éventuellement des pièces jointes. Au moment de l'envoi, thunderbird coté émetteur réalise les opérations suivantes :

Avec un algorithme (exemple : md5sum[4], RSA[5]), thunderbird calcule une empreinte du courriel. La probabilité d'avoir deux empreintes semblables pour deux courriels différents est si faible qu'elle est considérée comme nulle. Cette empreinte est chiffrée avec la clé privée et transmise avec le courriel.

3 https://keys.openpgp.org/
4 https://fr.wikipedia.org/wiki/Md5sum
5 https://fr.wikipedia.org/wiki/Chiffrement_RSA

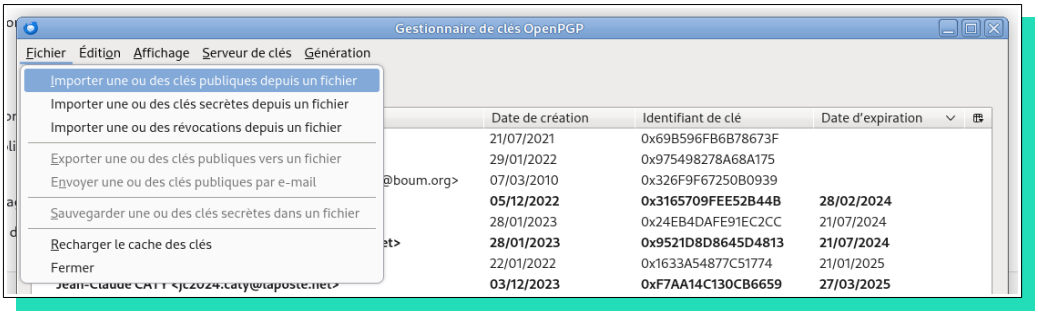
Coté récepteur, le courriel est reçu. Thunderbird calcule l'empreinte de ce courriel avec le même algorithme que celui de l'émetteur. Parallèlement, l'empreinte chiffrée transmise dans le courriel est déchiffrée avec la clé publique de l'émetteur (grâce à l'interchangeabilité des clés). L'empreinte calculée et l'empreinte déchiffrée sont comparées. La signature est validée si ces deux empreintes sont identiques.

Opérations sous thunderbird

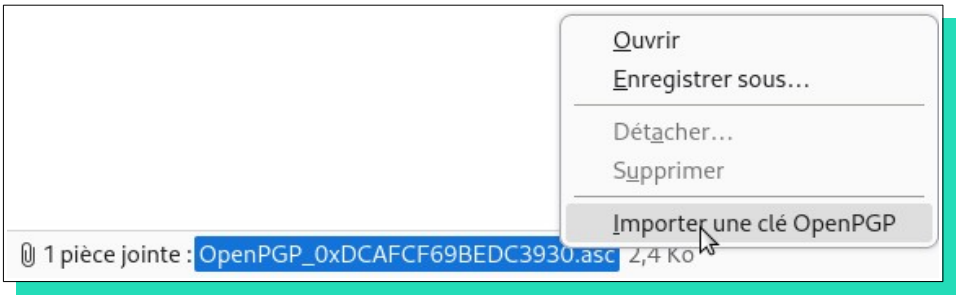
Réception d'une clé publique

Vous souhaitez transmettre votre clé publique pour que l'on puisse chiffrer les courriels qui vous sont destinés. Deux possibilités :

- Vous échangez votre clé en présentiel via une clé USB ou tout autre support. Votre interlocuteur va ouvrir son gestionnaire de clés via le menu « *Outils / Gestionnaire de clés openPGP* » de thunderbird. Il pourra l'importer via le menu « *Fichier /Importer une ou des clés publiques depuis un fichier* » du gestionnaire de clés.



- Vous recevez une clé comme pièce jointe d'un courriel. Un clic droit sur la pièce jointe vous offre la possibilité d'importer la clé



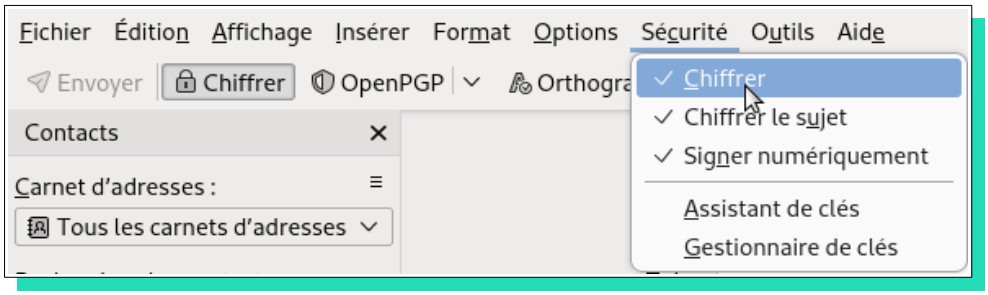
Attention cependant : si vous n'êtes pas certain de la provenance de ce courriel (il peut s'agir d'un courriel d'une personne que vous connaissez mais dont la boîte mail a été piratée), vous devez vérifier le certificat de la clé. Il faut également vérifier qu'un éventuel pirate de la boîte mail précité n'est pas celui qui aurait certifié la clé à la place de son vrai propriétaire … (un petit coup de fil sera peut être nécessaire) Si la clé a été enregistrée via l'outil de publication de thunderbird (vu plus haut), elle sera visible sur le site https://keys.openpgp.org/

Transmission d'une clé publique

Vous pouvez demander à thunderbird de joindre systématiquement votre clé publique dans chaque courriel envoyé. Via le menu « *Édition / paramètres des comptes* », option « *Chiffrement de bout en bout* », vous repérez la section « *Paramètres avancés* » et vous cochez « *Joindre ma clé publique …* ». Certifiez préalablement votre clé pour permettre à tout récepteur de vérifier son authenticité auprès de l'organisme de certification.

Chiffrer un courriel

Vous souhaitez chiffrer un courriel à l'attention d'un ou plusieurs de vos correspondants. Vous devez connaître la ou les clés publiques de ces correspondants et les avoir enregistrées dans votre gestionnaire de clés. Après avoir rédigé votre courriel, avoir éventuellement joint quelques pièces, vous demandez le chiffrement via l'option de menu « *Sécurité / Chiffrer* ». Via ce menu, vous pouvez également choisir ou non de chiffrer le sujet du courriel.



Signer un courriel

Via ce même menu, vous constatez que vous pouvez également signer vos courriels. Cette option (comme celles de chiffrement) sont des bascules « *on/off* ». Les options cochées resteront cochées pour les envois suivants.

Propriétés d'une clé

Précédemment, nous avons vu le gestionnaire de clés. Ce dialogue offre la possibilité d'afficher et modifier les propriétés d'une clé. Après avoir sélectionné une clé, nous pouvons afficher ses propriétés via l'option de menu « *Affichage / Propriétés d'une clé* ». Il est alors possible de :

- Préciser la confiance accordée à cette clé dans l'onglet « *Votre acceptation* »,
- d'afficher la *certification* de la clé,

- de connaître la *structure* de la clé, par exemple algorithme de création et date d'expiration de la clé.